ABSTRACT OF THE DISCLOSURE

CRC DATA PROTECTION SCHEME FOR NON-BLOCK-ORIENTED DATA

A hardware-controlled data protection scheme can be used on a device providing buffering between two different protocols, especially where at least one of the protocols does not use fixed length blocks. A fixed block size is arbitrarily imposed on the data in order to calculate a cyclical redundancy code (CRC) for the block. Block sizes are restricted to a value of 2^n, e.g., 2, 4, 8, 16, etc. The device is able to time-share and to receive or send data on more than one port while sharing the CRC engine between the ports. Intermediate values of the CRC for a given port are temporarily saved in a CRC register file. As a block of data for a given port is completed, a final CRC value for the block is saved to a CRC random access memory (RAM) located on the device and the entry in the register file is cleared. When the data is then output from the device, the CRC for the block is recalculated and checked against the saved value to be sure that they match.